

REMARKS

Applicants have considered the outstanding official action. It is respectfully submitted that the claims are directed to patentable subject matter and are in condition for allowance as set forth below.

Applicants have added an abstract of disclosure on a separate sheet as required.

Claims 5-12 and 16 are objected to under 37 CFR 1.75(c) as being in improper multiple dependent form.

Applicants have amended the claims to correct the dependencies.

Claims 1-16 are rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,389,538 (Gruse).

Claim 1 is the only independent claim. Claim 1 claims a device for secure transmission respectively forwarding of coded data from a first data station via a second data station to a third data station of a network, comprising an input unit for receiving the coded data from the first data station and for receiving a requester's external key from the third data station or a further data station; a unit for recoding the coded data by means of decoding with an internal key and renewed encoding with the

external key, with the internal key not being accessible from outside the device; and an output unit for issuing the data encoded with the external key, wherein the device is designed in such a manner on or in the second data station that the unit for recoding recodes the data only upon request by the third data station with aid of the requester's external key and the data are not accessible in decoded form on the second data station from outside the device.

Claim 12 claims a process for secure data transmission of data from a first data station via a second data station to a third data station using the device according to claim 1, on or in the second data station, comprising steps of: encoding the data in the first data station with a first key; dividing the first key into a first part and a second part in such a manner that neither the first part nor the second part alone permit decoding the coded data; encoding the first part of the first key in the first data station with a public key of the second data station; transmitting the coded data together with the coded first part of the first key to the second data station; storing the coded data and the coded part of the first key in the second data station; requesting the data by the third

data station, identity of which is not conveyed to the second data station until requested; decoding the coded part of the first key with a private key of the second data station matching the public key and recoding previously decoded part of the first key with a public key of the third data station; transmitting the coded data together with the recoded first part of the first key to the third data station; decoding the coded first part of the first key in the third station with a private key matching the public key of the third station; completing the first key in the third data station by adding the first part to the second part of the first key which was transmitted on a separate path from the first data station to the third data station, and decoding the coded data with the complete first key in the third data station.

Gruse teaches a system for distribution of digital content, e.g., print media, films, music over global communication networks such as the Internet or World Wide Web and tracking the usage of the digital content on user devices to manage the rights of the asset owners. The system has the following functional elements: Content Provider(s), Electronic Digital Content Store(s), Intermediate Market Partner(s), Clearinghouse(s), End-User

Device(s) and Transmission Infrastructure(s). The system provides for distribution of digital content over a network from the Content Provider(s) via the Electronic Digital Content Store(s) to finally the End-User Device(s), licensing authorization and control so that the content is unlocked only by authorized intermediate or End-User(s) that have secured a license, and control and enforcement of content usage according to the conditions of purchase or license, such as permitted number of copies, number of plays, and the time interval or term the license may be valid. Information and the content is distributed among the system components in coded form using cryptographic carriers, so called Secure Containers that use encryption, digital signatures, and digital certificates to provide protection against unauthorized interception or modification of electronic information and content.

The Clearinghouse(s) receives from an End-User Device the public key of the End-User Device as one input and the Order Secure Containers containing, among other things, the encrypted symmetric key, i.e., coded data, as another input. The Clearinghouse(s) verifies and validates the information provided in the Order Secure Containers. Once all the checks are successfully completed, the

encrypted symmetric key is decrypted using the private key of the Clearinghouse(s). The symmetric key is then encrypted using the public key of the End-User. This new encrypted symmetric key is then packaged into a License Secure Container and sent to the End-User.

Gruse does not teach or disclose the explicit data handling inside the Clearinghouse(s). Gruse does not teach or disclose anything about the data handling in a special secure device in or at the Clearinghouse, which assures that the private key of the Clearinghouse is not accessible from outside the device as in the claimed invention. For a person skilled in the art, Gruse does not teach or disclose any explicit or implicit information or details to provide or suggest any motivation to modify the teachings of Gruse to provide the claimed invention.

Additionally, with regard to rejected process/method claims 12-16, the encoding of data, i.e., the encoding of the electronic content with a symmetric key and the encoding of the symmetric key with the public key of the Clearinghouse, is performed at the Content Provider. Gruse does not teach or suggest providing a partial encoding of the symmetric key with the public key of the Clearinghouse as in the claimed invention. Gruse further teaches, in

contrast to the claimed invention, that the coded data are not sent together from the Content Provider to a second data station, but separately to different data stations. Thus, Gruse teaches that the encoded content is sent to a Content Hosting Site and the encoded symmetric key is sent among other data to an Electronic Digital Content Store.

Additionally, in contrast to the claimed invention, following a request from a third data station, the decoding of the symmetric key and the recoding of the symmetric key with the public key of the third station neither takes place in the Content Hosting Site nor the Electronic Digital Content Store. Instead, Gruse teaches the transfer of the encoded symmetric key from the Content Provider via the Electronic Digital Content Store and the End-User Device to the Clearinghouse before the recoding of the symmetric key with the public key of the End-User is performed.

Accordingly, Gruse does not teach or suggest each and every element of the claimed invention. Withdrawal of the §102 rejection is respectfully requested.

Reconsideration and allowance of the claims are respectfully requested.

5551/PCT/USSN 09/937,819
Group Art Unit 2131

Respectfully submitted,

VOLKER PAUL ET AL

By Mary Breiner
Mary J. Breiner, Attorney
Registration No. 33,161
BREINER & BREINER, L.L.C.
115 North Henry Street
P.O. Box 19290
Alexandria, Virginia 22320-0290

Telephone: (703) 684-6885